Select a profile by clicking on it to highlight it and then click on the `OK` button to exit the window. The `SECURITY MANAGER:Assign Applications to Profiles` window (Figure 21) returns to the forefront.

STEP 4: **Assign one or more applications to the profile, if desired**. After you select a profile, assigned applications for that profile appear in the `Assigned Applications` column and available applications for that profile appear in the `Available Applications` column. Assign one or more applications to the profile, if desired, by highlighting the applications in the `Available Applications` column. Once highlighted, the applications move to the `Assigned Applications` column.

STEP 5: **De-assign one or more applications to the profile, if desired**. De-assign one or more applications to the profile, if desired, by highlighting the applications in the `Assigned Applications` column. Once highlighted, the applications move to the `Available Applications` column.

STEP 6: **Apply your changes**. Click on the `Apply` button to apply your changes and remain in the window, or click on the `OK` button to apply your changes and exit the `SECURITY MANAGER:Assign Applications to Profiles` window. If you choose to click on the `Apply` button instead of the `OK` button, you can continue to assign applications to different profiles, if desired, and apply your changes for each profile without exiting the window until you are finished.

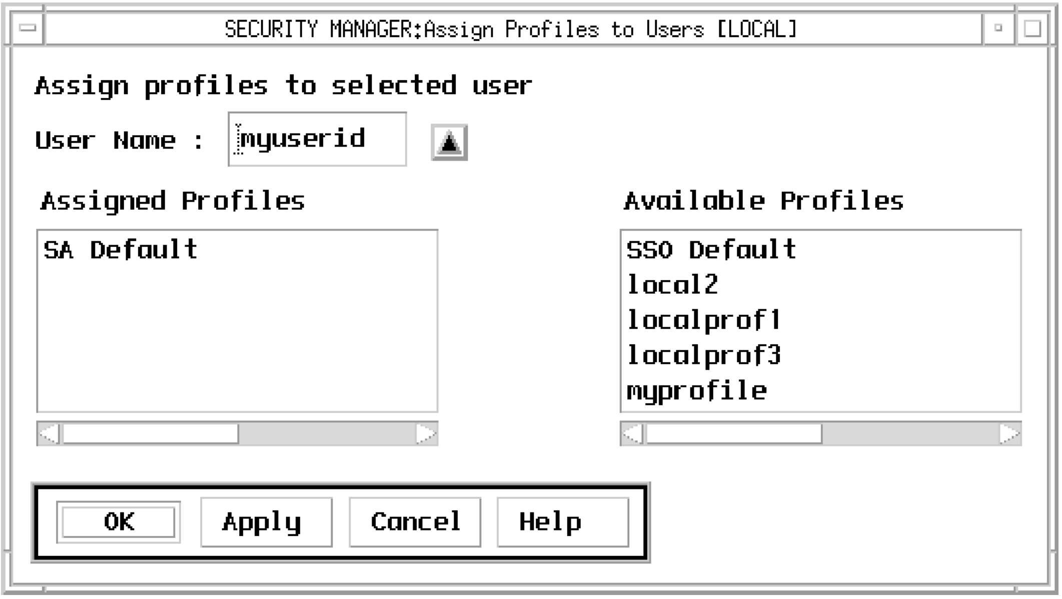
3.3.4 Assigning Profiles to Users

Follow the steps below to assign profiles to users.

NOTE: In the current release, local profiles can only be assigned to local users. Similarly, global profiles can only be assigned to global users.

STEP 1: **Open the `SECURITY MANAGER:Profile Manager` window**. Open the `SECURITY MANAGER:Profile Manager` window (Figure 17), as described in Section 3.3, *Profile Management.*

STEP 2: **Choose to assign profiles to a user**. Select the `Assign to User` option from the `Profile` pull-down menu. The `SECURITY MANAGER:Assign Profiles to Users` window appears (Figure 23).


SECURITY MANAGER:Assign Profiles to Users [LOCAL]
Assign profiles to selected user
Assigned Profiles
Available Profiles
OK
Apply
Cancel
Help

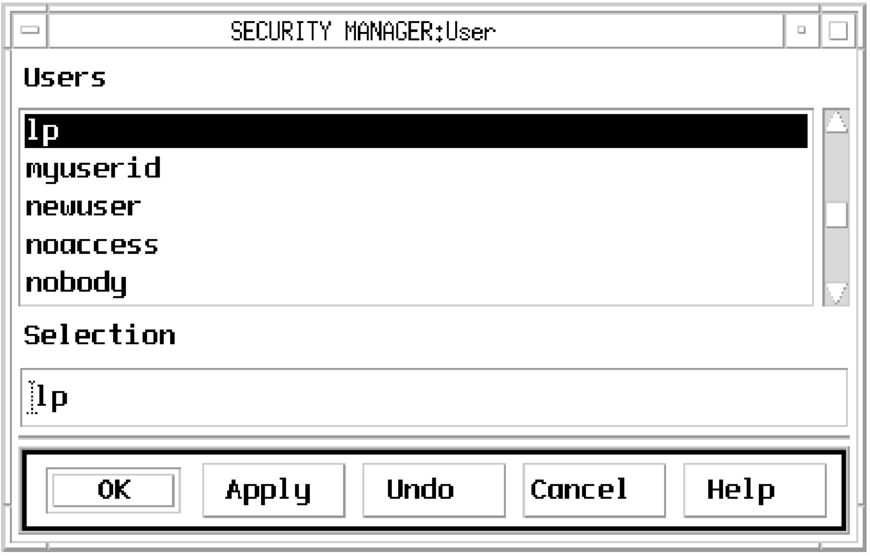
User Name : myuserid

Assigned Profiles:
SA Default

Available Profiles:
SSO Default
local2
localprof1
localprof3
myprofile

Figure 23. SECURITY MANAGER:Assign Profiles to Users Window

STEP 3: Use the `User Name` toggle to select a user name in the `User Name` field. The `SECURITY MANAGER:User` window appears (Figure 24). This window lists all user names.



Users:
lp
myuserid
newuser
noaccess
nobody

Selection: lp

Figure 24. SECURITY MANAGER:User Window

Select a user account by clicking on it to highlight it and then click on the `OK` button to exit the window. The `SECURITY MANAGER:Assign Profiles to Users` window (Figure 23) returns to the forefront.

STEP 4: **Assign one or more profiles to the user account, if desired**. After you select a user account, assigned profiles for that user account appear in the `Assigned Profiles` column and available profiles for that user account appear in the `Available Profiles` column. Assign one or more profiles to the user account, if desired, by highlighting the profiles in the `Available Profiles` column. Once highlighted, the profiles move to the `Assigned Profiles` column.

STEP 5: **De-assign one or more profiles to the user account, if desired**. De-assign one or more profiles to the user account, if desired, by highlighting the profiles in the `Assigned Profiles` column. Once highlighted, the applications move to the `Available Profiles` column.

STEP 6: **Apply your changes**. Click on the `Apply` button to apply your changes and remain in the window, or click on the `OK` button to apply your changes and exit the `SECURITY MANAGER:Assign Profiles to Users`window. If you choose to click on the `Apply` button instead of the `OK` button, you can continue to assign profiles to different users, if desired, and apply your changes for each user without exiting the window until you are finished.

NOTE: Profiles assigned to users are available for the user in the `Profile Selector` window. In addition, selected profiles appear as folders within the `Application Manager` window. Reference Section 8.1, *Enabling and Disabling the Profile Selector*, for more information about launching the `Profile Selector` window after successful user login.

4. Text Editing

The `Edit` menu in the `SECURITY MANAGER` window contains options to cut, copy, and paste selected text from one field to another, as well as to delete selected text. Text can be cut, copied, pasted, or deleted from any text field that requires user input in any user window.

4.1 Cutting Text

Follow the steps below to cut text from one text input field so it can be pasted into another text input field.

STEP 1: **Highlight the text you want to cut**. Use the mouse to highlight the text you want to cut from a text input field in a user window.

STEP 2: **Bring the `SECURITY MANAGER` window to the forefront**. Click on the `SECURITY MANAGER` window (Figure 3) to bring it to the forefront.

STEP 3: **Choose to cut the text**. Select `Cut` from the `Edit` pull-down menu in the `SECURITY MANAGER` window. The text that was cut no longer appears in the text input field. Follow the steps in subsection 4.3, *Pasting Text*, to paste the text in another text input field.

4.2 Copying Text

Follow the steps below to copy text from one text input field into another text input field.

STEP 1: **Highlight the text you want to copy**. Use the mouse to highlight the text you want to copy from one text input field in one user window to another text input field in the same window or in another window.

STEP 2: **Bring the `SECURITY MANAGER` window to the forefront**. Click on the `SECURITY MANAGER` window (Figure 3) to bring it to the forefront.

STEP 3: **Choose to copy the text**. Select `Copy` from the `Edit` pull-down menu in the `SECURITY MANAGER` window. Follow the steps in subsection 4.3, *Pasting Text*, to paste the text in another text input field.

4.3 Pasting Text

Follow the steps below to past text from one text input field into another text input field.

STEP 1: **Choose to cut or copy the text you want to paste**. Follow the steps in subsection 4.1, *Cutting Text*, or subsection 4.2, *Copying Text*, to cut or copy text from one text input field that you want to paste in another text input field.

STEP 2: **Choose where you want to paste the cut or copied text**. Place your cursor in the text input field in which you want to paste the cut text.

STEP 3: **Bring the `SECURITY MANAGER` window to the forefront**. Click on the `SECURITY MANAGER` window (Figure 3) to bring it to the forefront.

STEP 4: **Choose to paste the text**. Select `Paste` from the `Edit` pull-down menu in the `SECURITY MANAGER` window. The pasted text appears in the text input field.

4.4 Deleting Text

Follow the steps below to delete text.

STEP 1: **Highlight the text you want to delete**. Use the mouse to highlight the text you want to delete from a text input field in a user window.

STEP 2: **Bring the `SECURITY MANAGER` window to the forefront**. Click on the `SECURITY MANAGER` window (Figure 3) to bring it to the forefront.

STEP 3: **Choose to delete the text**. Select `Delete` from the `Edit` pull-down menu in the `SECURITY MANAGER` window. The deleted text no longer appears in the text input field.

5. Account Scope

The current scope of the Security Manager session is displayed in the title bar of all Security Manager windows as either [LOCAL] or [GLOBAL]. The default scope is [LOCAL] when Security Manager is started on the workstation.

Changing the scope changes the source of the information available to Security Manager as follows:

When the scope is Local:

User Accounts:	/etc/passwd
UNIX Groups:	/etc/group
User Directories:	/h/USERS/local
Profile Database:	/h/USERS/local/Profiles

When the scope is Global:

User Accounts:	NIS or NIS+ passwd database
UNIX Groups:	NIS or NIS+ group database
User Directories:	/h/USERS/global
Profile Database:	/h/USERS/global/Profiles

To change the scope of the Security Manager session, select the Option menu from the main menu bar. The Option menu contains the following options: Local Accounts, Remote Accounts, and Global Accounts. These options can be used to determine if a user account will be local, remove, or global. These options are described in the following subsections.

NOTE: Exiting and restarting Security Manager resets the scope to [LOCAL].

5.1 Local Accounts

The Local Accounts option is used to create or modify a user account on the user's workstation.

5.2 Remote Accounts

The Remote Accounts option is used to give a user access to a local user account on one workstation from a second workstation.

5.3 Global Accounts

The `Global Accounts` option is used to create or modify a user account for all workstations in the NIS/NIS+ domain.

The `Global Accounts` option cannot be used unless a workstation is configured for NIS/NIS+. `Global Accounts` will be disabled on stand-alone workstations. On a NIS client, `Global Accounts` will be available for viewing, but modifying the accounts or groups is not allowed. On a NIS or NIS+ server or on a NIS+ client added to the administration group, full global account functionality is available. A NIS client will be able to use global accounts if it mounts `/h/USERS/global` from the NIS master. Reference the *DII COE System Administrator's Guide (HP-UX 10.20 and Solaris 2.5.1)* for more information about NIS.

NOTE: Only the `secman` account should create global users and profiles.

6. Secman Password Management

Follow the steps below to change the secman password.

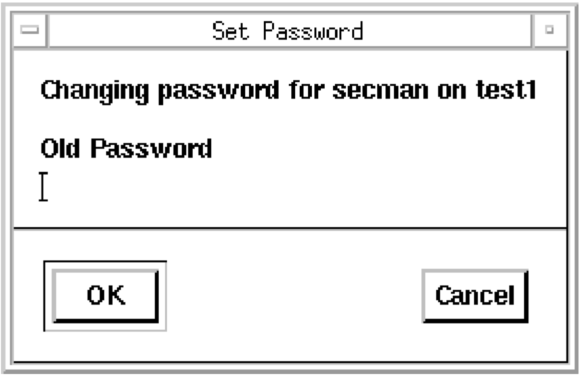
STEP 1: **Log in as secman**. Type secman at the Name prompt and press [RETURN].

STEP 2: **Enter the secman password**. Type the secman password at the Password prompt and press [RETURN]. The Security Administration software appears.

STEP 3: **Access the Application Manager**. Double-click on the Application Manager control on the CDE Front Panel to open the Application Manager window.

STEP 4: **Select the DII_TOOLS folder**. Double-click on the DII_TOOLS folder in the Application Manager window to open the Application Manager - DII_TOOLS folder.

STEP 5: **Select the Chg Password icon**. Double-click on the Chg Password icon to open the Set Password window (Figure 25).



Changing password for secman on test1

Old Password

Figure 25. Set Password Window

STEP 6: **Enter the current secman password**. Enter the current secman password in the Old Password field and click on the OK button.

STEP 7: **Enter the new secman password**. The New Password window appears. Enter the new secman password in the Enter New Password field and click on the OK button.

STEP 8: **Verify the new secman password**. The Verify New Password window appears. Enter the new secman password in the field and click on the OK button.

STEP 9: **Acknowledge that the secman password has changed**. Click on the OK button when the following message appears:

```
Your password has been successfully updated!
```

This page intentionally left blank.

7. Profile Modification

Once created and defined, profiles can be modified to add and restrict access to functions within menus and options using the `Edit Profiles` icon. Follow the steps below to modify profiles.

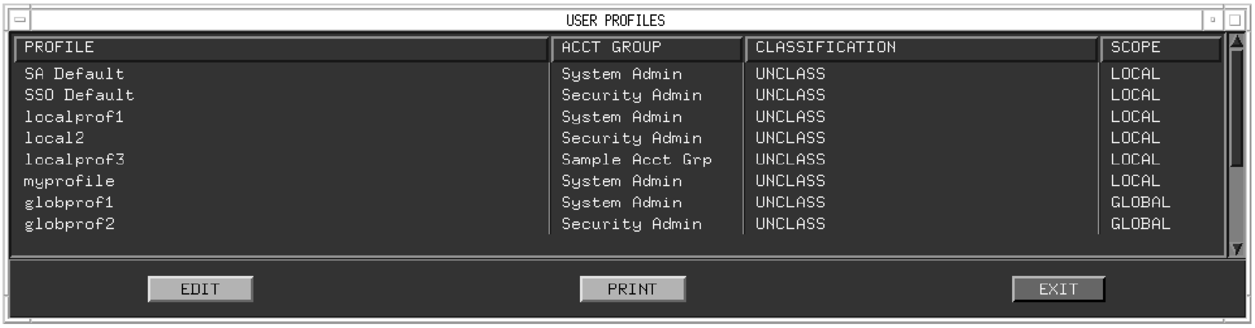
STEP 1: **Log in as `secman`**. Type `secman` at the `Name` prompt and press [RETURN].

STEP 2: **Enter the `secman` password**. Type the `secman` password at the `Password` prompt and press [RETURN]. The Security Administration software appears.

STEP 3: **Access the Application Manager**. Double-click on the Application Manager control on the CDE Front Panel to open the `Application Manager` window.

STEP 4: **Select the `DII_APPS` folder**. Double-click on the `DII_APPS` folder in the `Application Manager` window to open the `Application Manager - DII_APPS` folder.

STEP 5: **Select the `Edit Profiles` icon**. Double-click on the `Edit Profiles` icon to open the `USER PROFILES` window (Figure 26). The `USER PROFILES` window lists all user profiles that can be modified.

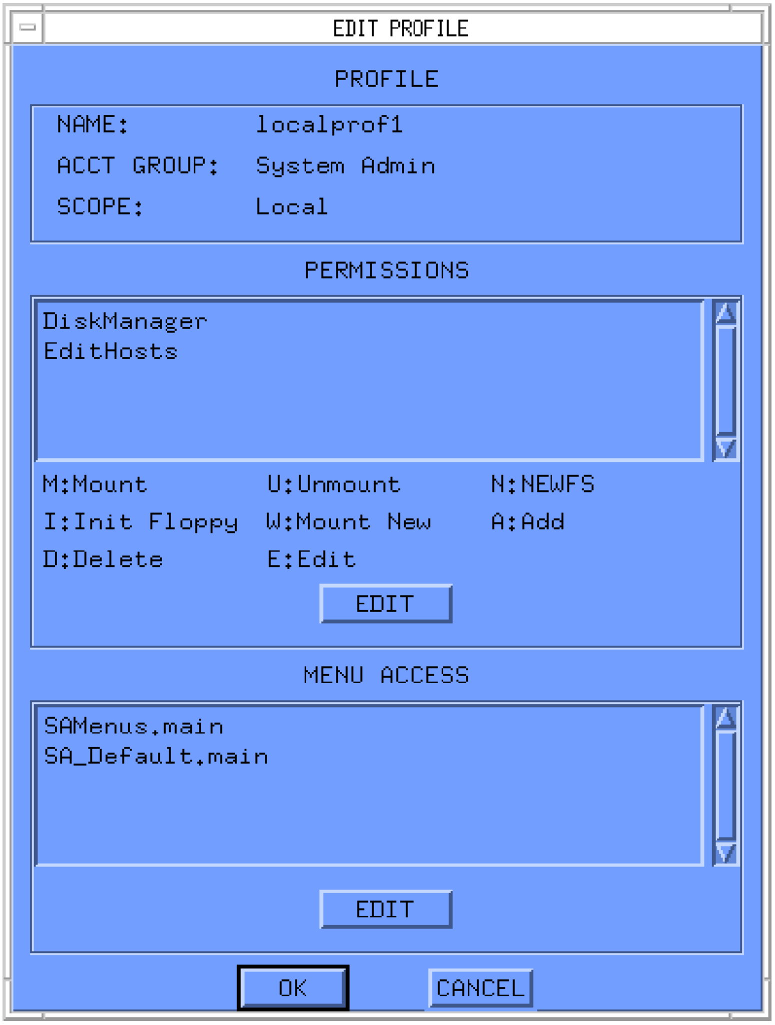


PROFILE	ACCT GROUP	CLASSIFICATION	SCOPE
SA Default	System Admin	UNCLASS	LOCAL
SSO Default	Security Admin	UNCLASS	LOCAL
localprof1	System Admin	UNCLASS	LOCAL
local2	Security Admin	UNCLASS	LOCAL
localprof3	Sample Acct Grp	UNCLASS	LOCAL
myprofile	System Admin	UNCLASS	LOCAL
globprof1	System Admin	UNCLASS	GLOBAL
globprof2	Security Admin	UNCLASS	GLOBAL

Figure 26. USER PROFILES Window

STEP 6: **Select the profile you want to modify**. To modify a profile's access to functions within menus and options, click on the profile to select it and click on the `EDIT` button.

STEP 7: **Review the information in the `EDIT PROFILE` window**. The `EDIT PROFILE` window appears (Figure 27). The `PERMISSIONS` panel shows the applications that have been assigned to that profile.



```
NAME:          localprof1
ACCT GROUP:    System Admin
SCOPE:         Local
```

```
DiskManager
EditHosts
```

```
M:Mount          U:Unmount     N:NEWFS
I:Init Floppy    W:Mount New   A:Add
D:Delete         E:Edit
```

```
SAMenus.main
SA_Default.main
```

Figure 27. EDIT PROFILE Window

STEP 8: **Modify permissions, if desired**. Highlight an option in the `PERMISSIONS` panel and click on the `EDIT` button to modify permission settings for the option. For example, in the `EDIT PROFILE` window (Figure 27), click on the `DiskManager` option and click on the `EDIT` button.

STEP 9: **Set permissions for the option**. The `EDIT PERMISSIONS` window appears (Figure 28). Figure 28 shows `DISKMANAGER PERMISSIONS` because the `DiskManager` option was selected in STEP 8. Click on the options for which the profile should have permissions. For example, if you want the profile to be able to mount a file system and unmount a file system, you would click on the `Mount` and `Unmount` toggles in Figure 28. Click on the `OK` button when you are done. The `EDIT PROFILE` window returns to the forefront.

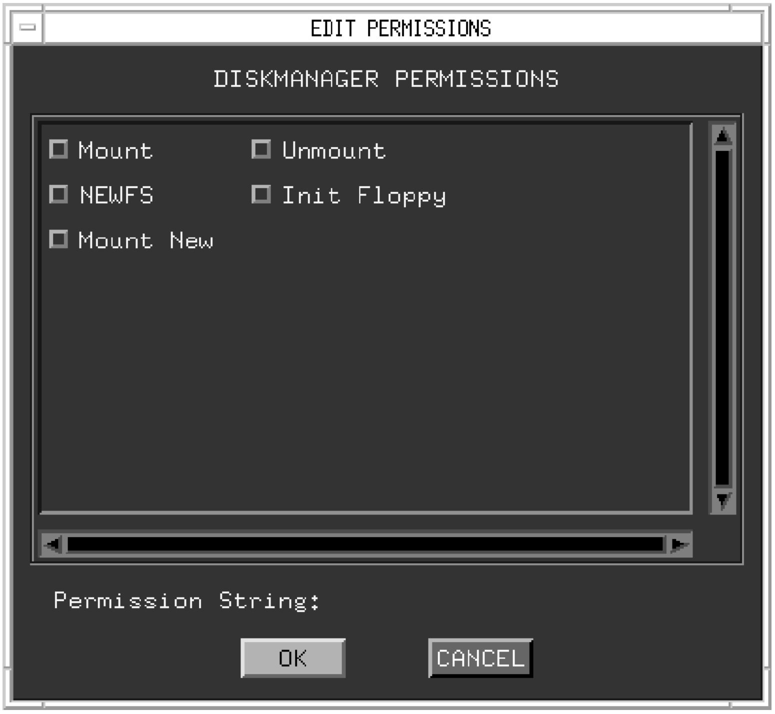


Figure 28. EDIT PERMISSIONS Window

STEP 10: **Modify menu access, if desired**. Highlight a menu in the `MENU ACCESS` panel and click on the `EDIT` button to modify menu access settings for the option. For example, in the `EDIT PROFILE` window (Figure 27), click on the `SAMenus.main` option and click on the `EDIT` button.

STEP 11: **Set menu access settings**. The `EDIT MENU ACCESS` window appears (Figure 29). Figure 29 shows System Administration menus because the `SAMenus.main` option was selected in STEP 10. Click on the menus for which the profile should have permissions. For example, if you want the profile to have access to the `Help` menu and the `SA System` menu, you would click on the `Help` and `SA System` toggles in Figure 29. Click on the `OK` button when you are done. The `EDIT PROFILE` window returns to the forefront.

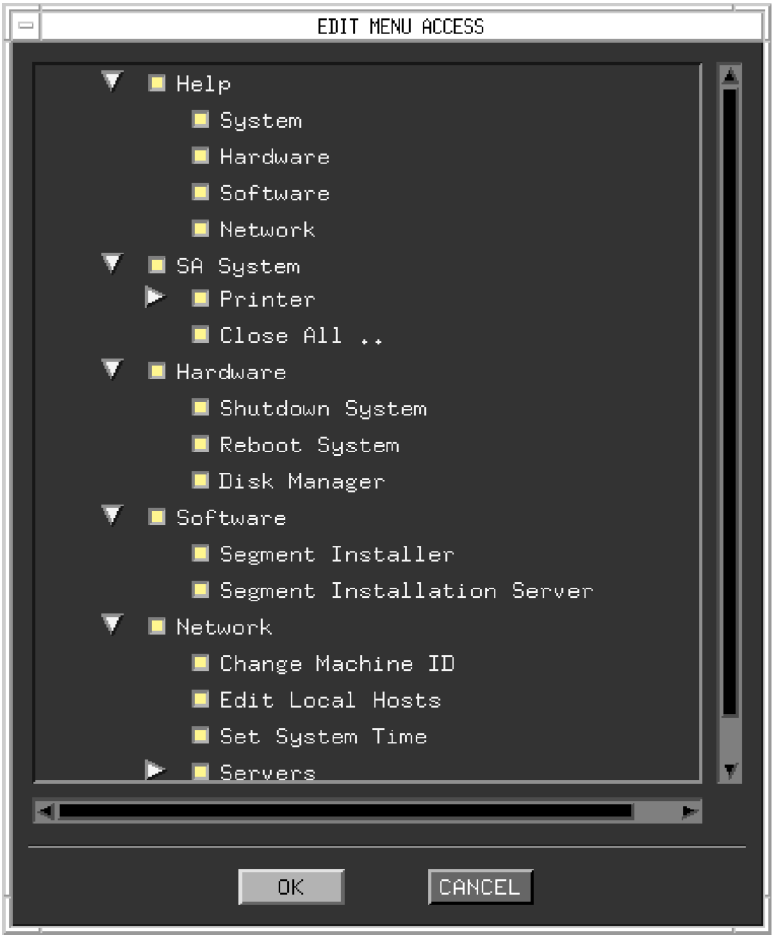


Figure 29. EDIT MENU ACCESS Window

STEP 12: **Apply your changes**. Click on the `OK` button in the `EDIT PROFILE` window (Figure 27) to apply your changes and exit the window.

8. Profile Configuration

The `Profile Configuration` icon contains options to manage audit status and audit logs on the workstation. Follow the steps below to access the `Profile Configuration` icon.

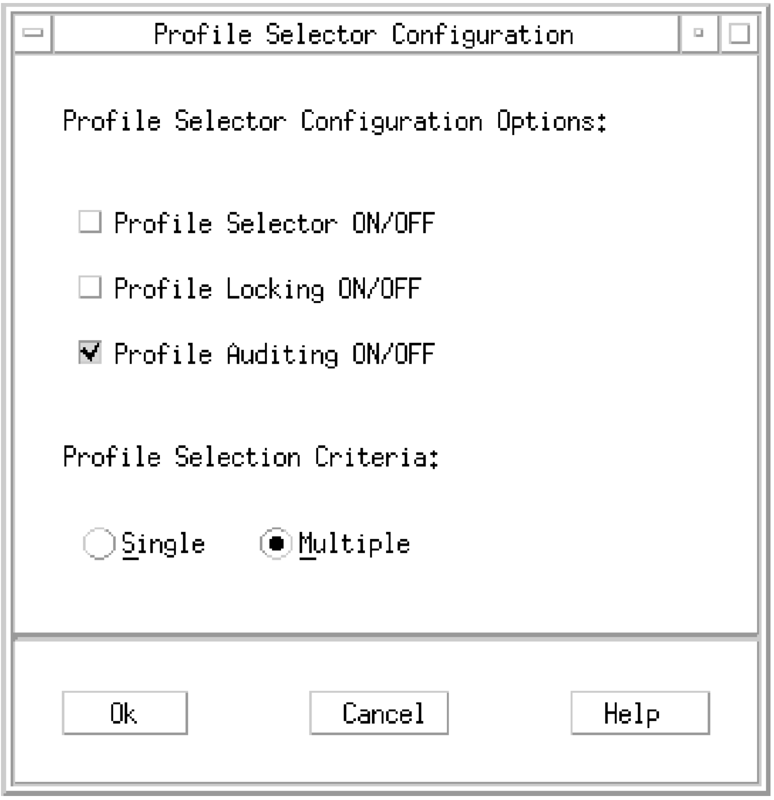
STEP 1: **Log in as `secman`**. Type `secman` at the `Name` prompt and press [RETURN].

STEP 2: **Enter the `secman` password**. Type the `secman` password at the `Password` prompt and press [RETURN]. The Security Administration software appears.

STEP 3: **Access the Application Manager**. Double-click on the Application Manager control on the CDE Front Panel to open the `Application Manager` window.

STEP 4: **Select the `DII_TOOLS` folder**. Double-click on the `DII_APPS` folder in the `Application Manager` window to open the `Application Manager - DII_APPS` folder.

STEP 5: **Select the `Profile Selector Config` icon**. Double-click on the `Profile Selector Config` icon to open the `Profile Selector Configuration` window (Figure 30).



Profile Selector Configuration

Profile Selector Configuration Options:

□ Profile Selector ON/OFF

□ Profile Locking ON/OFF

☑ Profile Auditing ON/OFF

Profile Selection Criteria:

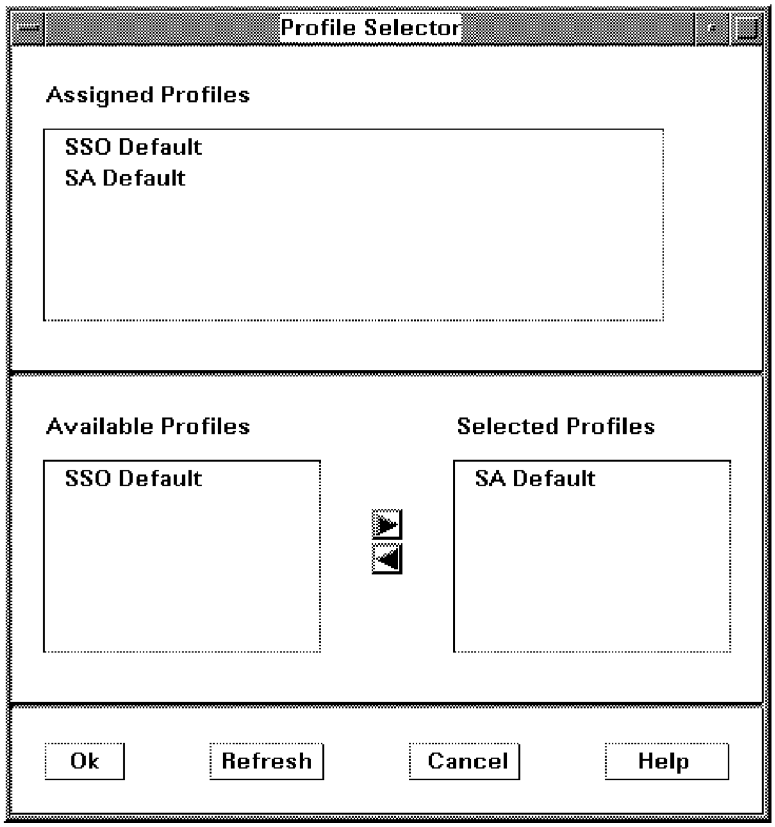
○ Single ● Multiple

Figure 30. Profile Selector Configuration Window

The `Profile Configuration` icon has four options: `Profile Selector On/Off`, `Profile Locking`, `Profile Auditing On/Off`, and `Profile Selection Criteria`.

8.1 Enabling and Disabling the Profile Selector

The `Profile Selector ON/OFF` function determines if the `Profile Selector` window (Figure 31) launches after successful user login if the user has multiple profiles. This option has no effect if the `Profile Locking` function is turned on.



Assigned Profiles: SSO Default, SA Default

Available Profiles: SSO Default

Selected Profiles: SA Default

Figure 31 Profile Selector Window

The `Profile Selector` window shows the profiles to which the user is assigned in the `Assigned Profiles` panel; the profiles that are available for the user in the `Available Profiles` panel; and the profile or profiles that have been selected in the `Selected Profiles` panel. If a user account has multiple profiles assigned to it and if the system administrator has enabled multiple profile selection (see Section 8.4, *Enabling and Disabling Single and Multiple Profile Selection Criteria*), the `Profile Selector` window will allow the user to choose multiple profiles as selected profiles. Regardless of whether or not the user account has multiple profiles assigned to it, if the system administrator has not enabled multiple profile selection, the `Profile Selector` window will only allow the user to choose one profile as the selected profile.

8.2 Enabling and Disabling Profile Locking

The `Profile Locking ON/OFF` function allows an administrator to restrict the occupancy of a profile to one user in an administrative domain (e.g., the capability to lock a profile on a profile-by-profile basis).

8.3 Enabling and Disabling Profile Auditing

The `Profile Auditing ON/OFF` function determines that an audit log will be written to the system's logs when a user selects or deselects any profile.

8.4 Enabling and Disabling Single and Multiple Profile Selection Criteria

The `Profile Selection Criteria` function allows a configurable number of selections, where the user may be restricted to selecting one profile only (`Single`) or can select many profiles (`Multiple`) (e.g., the total number of valid profiles for that particular user). Once you choose to enable multiple profiles, you no longer have the capability to enable single profiles.

This page intentionally left blank.